Exhibit A

Store	Mac	iPad	iPhone	Watch	TV	Music	Support			

Newsroom

Search Newsroom   Popular Topics ∨

UPDATE

May 11, 2021

App Store stopped more than $1.5 billion in potentially fraudulent transactions in 2020

Apple helps keep the App Store a safe and trusted place for users to discover apps by detecting and taking action against fraudulent developers and users.

Threats have been present since the first day the App Store launched on iPhone, and they've increased in both scale and sophistication in the years since. Apple has likewise scaled its efforts to meet those threats, taking relentless steps forward to combat these risks to users and developers alike.

It takes significant resources behind the scenes to ensure these bad actors can't exploit users' most sensitive information, from location to payment details. While it's impossible to catch every act of fraud or ill intent before it happens, thanks to Apple's industry-leading antifraud efforts, security experts agree the App Store is the safest place to find and download apps.[1]

In 2020 alone, Apple's combination of sophisticated technology and human expertise protected customers from more than $1.5 billion in potentially fraudulent transactions, preventing the attempted theft of their money, information, and time — and kept nearly a million risky and vulnerable new apps out of their hands.

App Review

The App Review team is an essential line of defense, carefully reviewing every app and every update to ensure they adhere to the App Store's strong guidelines on privacy, security, and spam. The guidelines have changed over time to respond to new threats and challenges, with the goal of protecting users and providing them with the very best experience on the App Store.

Apple's goal is always to get new apps onto the store. In 2020, the team assisted more than 180,000 new developers in launching apps. Sometimes this takes a few tries. An app might be unfinished or not functioning properly when it's submitted for approval, or it might not yet have a sufficient mechanism for moderating user-generated content. In 2020, nearly 1 million problematic new apps, and an additional nearly 1 million app updates, were rejected or removed for a range of reasons like those.

A smaller but significant set of these rejections was for egregious violations that could harm users or deeply diminish their experience. In 2020 alone, the App Review team rejected more than 48,000 apps for containing hidden or undocumented features, and more than 150,000 apps were rejected because they were found to be spam, copycats, or misleading to users in ways such as manipulating them into making a purchase.

Some developers perform a bait and switch: fundamentally changing how the app works after review to evade guidelines and commit forbidden and even criminal actions. When such apps are discovered, they're rejected or removed immediately from the store, and developers are notified of a 14-day appeals process before their accounts are permanently terminated. In 2020, about 95,000 apps were removed from the App Store for fraudulent violations, predominantly for these kind of bait-and-switch maneuvers.

In just the last few months, for example, Apple has rejected or removed apps that switched functionality after initial review to become real-money gambling apps, predatory loan issuers, and pornography hubs; used in-game signals to facilitate drug purchasing; and rewarded users for broadcasting illicit and pornographic content via video chat.

Another common reason apps are rejected is they simply ask for more user data than they need, or mishandle the data they do collect. In 2020, the App Review team rejected over 215,000 apps for those sorts of privacy violations. Apple believes privacy is a fundamental right, and this commitment is a major reason why users choose the App Store.

Even with these stringent review safeguards in place, with 1.8 million apps on the App Store, problems still surface. Users can report problematic apps by choosing the Report a Problem feature on the App Store or calling Apple Support, and developers can use either of those methods or additional channels like Feedback Assistant and Apple Developer Support.
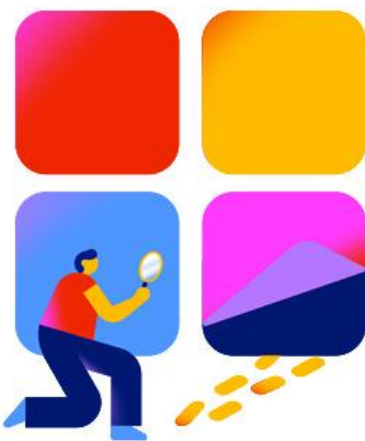
Fraudulent Ratings and Reviews

App Store ratings and reviews help many users make decisions about which apps to download, and developers rely on them to incorporate new features that respond to user feedback. Apple relies on a sophisticated system that combines machine learning, artificial intelligence, and human review by expert teams to moderate these ratings and reviews to help ensure accuracy and maintain trust. Since 2020, Apple has processed over 1 billion ratings and over 100 million reviews, and over 250 million ratings and reviews were removed for not meeting moderation standards.

Apple also recently deployed new tools to verify rating and review account authenticity, to analyze written reviews for signs of fraud, and to ensure that content from deactivated accounts is removed.

Account Fraud

Unfortunately, sometimes developer accounts are created entirely for fraudulent purposes. If a developer violation is egregious or repeated, the offender is expelled from the Apple Developer Program and their account terminated. Apple terminated 470,000 developer accounts in 2020 and rejected an additional 205,000 developer enrollments over fraud concerns, preventing these bad actors from ever submitting an app to the store.

Despite fraudsters' sophisticated techniques to obscure their actions, Apple's aggressive monitoring means these accounts are terminated, on average, less than a month after they are created.

Apple's work to ensure the safety of users who download apps extends even beyond the App Store. Over the last 12 months, Apple found and blocked nearly 110,000 illegitimate apps on pirate storefronts. These storefronts distribute malicious software often designed to resemble popular apps — or that modify popular apps without their developers' authorization — while circumventing the App Store's security protections.

And in just the last month, Apple blocked more than 3.2 million instances of apps distributed illicitly through the Apple Developer Enterprise Program. The program is designed to allow companies and other large organizations to develop and privately distribute internal-use apps to their employees that aren't available to the general public. Fraudsters attempt to distribute apps via this method to circumvent the rigorous App Review process, or to implicate a legitimate

enterprise by manipulating an insider to leak credentials needed to ship illicit content.

In addition to fraudulent developer accounts, Apple works to identify and deactivate fraudulent user accounts. In 2020 alone, Apple deactivated 244 million customer accounts due to fraudulent and abusive activity. In addition, 424 million attempted account creations were rejected because they displayed patterns consistent with fraudulent and abusive activity.

Payment and Credit Card Fraud

Financial information and transactions are some of the most sensitive data that users share online. Apple has invested significant resources in building more secure payment technologies like Apple Pay and StoreKit, which are used by more than 900,000 apps to sell goods and services on the App Store. For example, with Apple Pay, credit card numbers are never shared with merchants — eliminating a risk factor in the payment transaction process.

With online data breaches frustratingly common, these protections are an essential part of keeping users safe. But users may not realize that when their credit card information is breached or stolen from another source, fraudsters may turn to online marketplaces like the App Store to attempt to purchase digital goods and services that can be laundered or used for illicit purposes.

Apple focuses relentlessly on this kind of fraud as well. In 2020 alone, the fusion of sophisticated technology and human review prevented more than 3 million stolen cards from being used to purchase stolen goods and services, and banned nearly 1 million accounts from transacting again. In total, Apple protected users from more than $1.5 billion in potentially fraudulent transactions in 2020.

From App Review, to fraudulent account detection, to prevention of financial crimes, Apple works around the clock and behind the scenes to keep the App Store a safe and trusted place for users and developers alike.

Share article

1. nokia.com/networks/portfolio/cyber-security/threat-intelligence-report-2020; media.defense.gov

Press Contacts

10/8/21, 1:04 PM
App Store stopped over $1.5 billion in suspect transactions in 2020 - Apple
Case 4:20-cv-05640-YGR   Document 821-11   Filed 10/08/21   Page 6 of 6

Katie Clark Alsadder
Apple
kclarkalsadder@apple.com
(408) 974-9976

Fred Sainz
Apple
sainz@apple.com
(669) 227-0492

Apple Media Helpline
media.help@apple.com
(408) 974-2042

Latest News

UPDATE

Apple opens Developer Academy in Detroit to create new career opportunities

October 7, 2021

UPDATE

Apple unveils new resources for elementary school coding and inclusive app design

October 5, 2021

UPDATE

Apple Watch Series 7 orders start Friday, October 8

October 4, 2021

 Newsroom

The latest news and updates, direct from Apple.

[Read more ›](#)

 › Newsroom › App Store stopped over $1.5 billion in suspect transactions in 2020

Shop and Learn	Services	Apple Store	For Business	Apple Values
Mac	Apple Music	Find a Store	Apple and Business	Accessibility
iPad	Apple TV+	Shop Online	Shop for Business	Education
iPhone	Apple Fitness+	Genius Bar		Environment
Watch	Apple News+	Today at Apple	**For Education**	Inclusion and Diversity
TV	Apple Arcade	Apple Camp	Apple and Education	Privacy
Music	iCloud	Apple Store App	Shop for K–12	Racial Equity and Justice
AirPods	Apple One	Refurbished and Clearance	Shop for College	Supplier Responsibility
HomePod	Apple Card	Financing		
iPod touch	Apple Books	Apple Trade In	**For Healthcare**	**About Apple**
AirTag	Apple Podcasts	Order Status	Apple in Healthcare	Newsroom
Accessories	App Store	Shopping Help	Health on Apple Watch	Apple Leadership
Gift Cards			Health Records on iPhone	Career Opportunities
	Account			Investors
	Manage Your Apple ID		**For Government**	Ethics & Compliance
	Apple Store Account		Shop for Government	Events
	iCloud.com		Shop for Veterans and Military	Contact Apple